



PERU

# Data Protection Laws of the World

# Introduction



Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. In 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

## Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.



## Data protection laws

Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy, which was the basis for the creation of a law that specifically protects the use of personal data of any natural person and applies to both private and state entities.

The Personal Data Protection Law N° 29733 ('PDPL') was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP ('Regulation') was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.

However, it should be noted that a new Regulation to the PDPL was enacted through Supreme Decree 016-2024-JUS, dated November 30, 2024 ('New Regulation'). The New Regulation aims to enhance the protection of personal data under the PDPL by including improvements to contribute to the defense of the protection of personal data considering the rapid development of e-commerce, artificial intelligence, and similar digital technologies. The New Regulation will formally enter into force on March 30, 2025, except for some dispositions that will enter into force subsequently, and will replace the current Regulation. Likewise, this New Regulation includes new obligations (eg, designation of a data protection officer or the notification of security incidents).

Together, the PDLP and its Regulation are the primary data protection laws in Peru.

Further, enacted in 2001 and amended several times since then, Law N° 27489 regulates private risk centers and the protection of the owner's personal information. Law N° 27489 regulates activities related to risk centers and companies that handle:

- Information posing higher risks to individuals (eg, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
- Sensitive personal data (according to the PDPL)

## Definitions

### Definitions (prior to March 30, 2025)

#### Definition of Personal Data

Any information — regardless of whether numerical, alphabetic, graphic, photographic, acoustic — about personal habits or any other kind of information about an individual that identifies or may identify such individual by any reasonable means.

#### Definition of sensitive personal data

Is defined as Personal Data revealing information regarding an individual's

- Physical or emotional characteristics, facts or circumstances of their emotional or family life, as well as personal habits that correspond to the most intimate sphere
- Racial and ethnic origin
- Economic income, opinions or political, religious, philosophical or moral convictions
- Union membership, or
- Physical or mental health, to sexual life

Additionally, the following is also considered Sensitive Personal Data:

- Biometric data, including data derived from biometric data which by itself renders a data subject identifiable, and
- Other similar data that impacts the data subject's privacy in similar ways.

### Definitions (after March 30, 2025)

#### Definition of Personal Data

Any information — regardless of whether numerical, alphabetic, graphic, photographic, acoustic — about personal habits, location, online identifiers or any other information concerning physical, economic, cultural or social aspects regarding an individual that identifies or may be used to identify a specific individual by any reasonable means. Information is considered identifiable when the individual's identity can be directly or indirectly verified from the combination of data through means that can be reasonably used.

#### Definition of Sensitive Personal Data

Any information revealing or related to an individual's

- genetics
- biometrics
- neural data
- moral or emotional data

- sexual or family life
- personal habits regarding the most intimate sphere
- union membership
- physical or mental health, or

And other information affecting the individual's privacy in similar ways.

#### **Definition of Health-related Personal Data**

Is information concerning the past, present or predicted health, physical or mental, of an individual, including information derived from a medical act, the degree of disability, and genetic information.

## **National data protection authority**

The Directorate for the Protection of personal data, which is part of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data (NDPA), is the primary agency in charge of enforcing data protection matters.

The NDPA's current address is:

Scipion Llona 350  
Miraflores, L-18  
Lima  
Peru

#### Website

## **Registration**

The National Registry for the Protection of Personal Data (NRPDP) maintains information about personal databases of public or private ownership and publishes a list of such databases to facilitate individuals' exercise of their rights of access to information, rectification, cancellation, opposition and others regulated in the PDPL and its Regulation.

In addition, the NRPDP maintains records of:

- Communications of cross-border flow of personal data, and
- The sanctions, precautionary or corrective measures imposed by the NDPA

The holders of personal databases must register in the NRPDP providing the following information:

- The name and location of the personal database
- The purposes and the intended uses of the database
- The identification of the owner of the personal database

- The categories and types of personal data to be processed
- Collection procedures and a description of the system for processing personal data
- The technical description of the security measures
- The recipients of personal data transfers

The cross-border transfer of personal data must be notified to the NDPA, including the information required for the transfer of data and registration of the database.

## Data protection officers

There is currently no requirement to appoint a data protection officer in the private sector (only in the public sector). However, when a company registers its personal database with the NDPA, it can report that it has a Security Manager of that database.

However, the New Regulation introduces the requirement to appoint a Personal Data Officer under certain circumstances. Although it is expected that the NDPA will issue guidelines for further guidance on interpretation and interpretation of this new requirement, according to the New Regulation, this obligation applies to Data Controllers and Data Processors:

- Who are a public entities
- Who Process large volumes of Personal Data, either in quantity or type of data,
- Who undertake data Processing activities that involve the Processing of:
  - Personal Data for a large number of data subjects
  - Sensitive Personal Data as part of the entity's main activity or line of business
  - Personal Data leading to evident prejudice to the data subject's fundamental rights or freedoms

The requirement for entities to come into compliance with this new requirement is subject to varying grace periods, spanning from November 30, 2025 to November 30 2028, and are determined by the entity's annual revenue, as follows:

Company Type / Size	Annual Revenue	Grace Period
Large	Over S/ 12'305,000 (approx. USD 3'326,000).	November 30, 2025
Medium	Over S/ 9'095,000 (approx. USD 2' 500,000.00) and up to S/ 12'305,000 (approx. USD 3 '326,000).	November 30, 2026
Small	Over S/ 802,500 (approx. USD 217,000.00) and up	November 30, 2027

	to S/ 9'095.000 (approx. USD 2'500,000).	
Micro	Up to S/ 802,500.00 (approx. USD 217,000.00).	November 30, 2028

The Personal Data Officer must be appointed based on professional qualities and knowledge and expertise in personal data protection (which must be duly accredited). The Personal Data Officer may be internal or external to the company. Internal Personal Data Officers may perform additional functions within the company, subject to certain limitations and conditions.

The key responsibilities of a Personal Data Officer are to:

- Inform and advise of the obligations established by the provisions regarding data protection
- Verify and report on compliance with the applicable regulation, as well as on compliance with the policies of the data controller or data processor, including the assignment of responsibilities, awareness and training of personnel involved in processing operations, and audits to be carried out
- Cooperate with the NDPA for the performance of its purposes and attributions, and
- Act as a point of contact for the NDPA for issues related to the processing of personal data.

## Collection and processing

The collection and processing of personal data requires the data subject's prior, informed, express and unequivocal consent. The consent may be expressed through electronic means.

The collection and processing of sensitive personal data requires the data subject's prior, informed, express and unequivocal consent, and must be expressed in writing.

The data subject's consent is not necessary if any of the following are true:

- The data are compiled or transferred for the fulfillment of governmental agency duties
- The data are contained or destined to be contained in a publicly available source
- The data are related to credit standing and financial solvency, as governed by applicable law (Law N° 27489)
- A law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investment on Public Services (Law N° 27332), provided that the information supplied does not breach the user's privacy

- The data are necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship
- The data are needed to protect the health of the data subject, and data processing is necessary, in circumstances of risk, for prevention, diagnosis, and medical or surgical treatment, provided that the processing is carried out in health facilities or by professionals in health sciences observing professional secrecy
- The data are needed for public interest reasons declared by law or public health reasons (both must be declared as such by the Ministry of Health) or to conduct epidemiological studies or the like, as long as dissociation procedures are applied
- The data are dissociated or anonymized
- The data are used by a nonprofit organization with a political, religious, or trade union purpose, and refer to the data of its members within the scope of the organization's activities
- The data are necessary to safeguard the legitimate interest of the data subject or the data handler
- The data are being processed for purposes linked to money laundering and terrorist financing or others that respond to a legal mandate
- In the case of economic groups made up of companies that are considered subjects obliged to inform, the data is processed in accordance with the rules that regulate the Financial Intelligence Unit, so that they may share information with each other about their respective clients to prevent money laundering and financing of terrorism (as well as in other instances of regulatory compliance, establishing adequate safeguards on the confidentiality and use of the information exchanged)
- When the treatment is carried out in a constitutionally valid exercise of the fundamental right to freedom of information
- Others expressly established by law

If the data controller outsources the processing of the personal data to a third party (*ie*, a processor), such party must also comply with the relevant requirements of the PDLP (*eg*, to maintain personal data as confidential and to use the personal data only for the purposes authorized and modify inaccurate information).

Upon termination or expiration of the outsourcing agreement, the personal data processed must be deleted, unless the data subject provides express consent to do otherwise.

The processing of personal data by cloud services, applications and infrastructure is permitted, provided compliance with the provisions of the PDPL and its Regulation is guaranteed.

## Transfer of personal data

Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation.

Generally, data subject consent is required.

### **Cross-border transfers**

The transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels' to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:

- In accordance with international treaties in which Peru is a party
- For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
  - Terrorism
  - Drug trafficking
  - Money laundry
  - Corruption
  - Human trafficking, and
  - Other forms of organized crime
- When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
- Bank or stock transfers concerning transactions in accordance with the applicable law
- The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
- The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction
- Other exempt purposes established by the Regulations

For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.

As an alternative to the above mentioned “adequate transfer” requirement, a Data Controller may execute with a Data Processor (or other Data Controller) the standard contractual clauses already approved by the Peruvian Data Protection Authority, which include several obligations and declarations regarding the data transfer between the parties.

## Security

Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

Therefore, they must comply with, among others, the following security measures:

- Document and implement mechanisms for access management, identification and authentication procedures, biannual verification of privileges and use of mechanisms such as passwords, digital certificates and tokens
- Monitor and periodically review security measures and staff training according to their roles and responsibilities
- Document and implement the generation of legible and timely records of interactions with data, including for traceability purposes, account information, schedules, actions, among others. Such records should have a procedure for disposal, storage, transfer, destruction, a minimum retention of two years and secure disposal; and should be generated continuously and immediately
- Document and implement measures to prevent unauthorized access and reproduction of digital documents, and exclusive use of approved institutional systems and tools, and
- Implement at least: (i) controls to maintain secure areas, (ii) controls to maintain secure equipment inside and outside the facilities, and (iii) controls to ensure the generation of secure and continuous backup copies and their integrity verification. Taking as a reference the recommendations indicated in the “NTP-ISO/IEC 27001: 2022 Information Technology. Security Techniques. Information Security Systems. Requirements” in the current edition.

Likewise, with the entry into force of the New Regulation, the holder of the personal database shall implement a Security Document that must have a certain date. The Security Document must be updated and contain, as a minimum, the procedures for access management, privilege management and periodic verification of the privileges assigned to the information systems. This includes technological platforms, mobile applications, database engines, among others, used for the processing of personal data, as well as internal policies for the management and processing of personal data, which must consider the context and life cycle of the data.

Furthermore, NDPA has issued a Security Directive through the Directorial Resolution N° 019-2013-JUS/DGPDP (Security Directive), as an instrument that makes it possible for those actors who process personal data to act in accordance with the applicable law as

it provides guidance on the conditions, requirements and technical measures that shall be considered to comply with the applicable regulation.

## Breach notification

Currently, notification incidents are regulated by Emergency Decree 007-2020, which approves the Digital Trust Framework, with the intent to strengthen cybersecurity ('Emergency Decree'). A Digital Security Incident is defined under the Emergency Decree as an 'event or series of events that may compromise the trust, economic prosperity, protection of individuals and their personal data, the information, among other assets of the organization, through digital technologies.'

According to the Emergency Decree public administration entities, digital service providers in the financial sector, utilities (electricity, water and gas), healthcare and passenger transportation, internet service providers, and other providers of critical activities (economic and/or social activity whose interruption has serious consequences on the health and safety of citizens, on the effective functioning of essential services that maintain the economy, society and government, or affects the economic and social prosperity in general) as well as educational services must comply with the following: (a) notifying the National Centre for Digital Security (National Centre) about every digital security incident; and, (b) reporting and collaborating with the NDPA in case of a digital security incident that involves personal data. Notwithstanding the foregoing, once the New Regulation enters into force, a mandatory obligation regarding notification incidents will be in place.

According to the New Regulation, a security incident consists of any breach of security resulting in the destruction, loss, unlawful alteration of personal data or unauthorized communication or exposure to such data.

In the event that a personal data security incident results in the exposure of large volumes of personal data, in quantity or type of data, or that may affect a large number of persons or when it involves sensitive data or when there is an evident prejudice to other rights or freedoms of the holder of the personal data, the holder of the database must notify the NDPA at the latest within 48 hours after becoming aware of it or becoming aware of it. If the notification is made after 48 hours, it must include the reasons and evidentiary support for the delay.

The personal data security incident notification should identify and describe at a minimum the following:

- The nature of the personal data security incident, including, where possible, the types of data and the approximate number of data subjects affected
- The name and contact details of the Personal Data Officer or other points of contact where further information can be obtained
- The possible consequences of the personal data security incident, and
- The measures taken or proposed by the data controller to remedy the personal data security breach, including, if applicable, the measures taken to mitigate the possible negative effects.

It should be noted that this obligation remains even if the data controller considers that the incident has been remedied or resolved internally.

Likewise, the holder of the personal database who notices a personal data security incident that affects the holder of the same in other of his rights, must communicate it within 48 hours without undue delay, in simple and clear language for its understanding, as well as the measures adopted to mitigate its effects. If such communication takes longer than 48 hours, it must be accompanied by an indication of the reasons for such delay.

Furthermore, in the event that the Personal Data security incident takes place in and /or through the digital environment, the notification is made, in addition to the NDPA, to the National Center for its incorporation into the National Register of Digital Security Incidents in accordance with the provisions of the Emergency Decree.

Pursuant to Emergency Decree 007-2020, which approves the Digital Trust Framework, with the intent to strengthen cybersecurity ("Emergency Decree"), public administration entities, digital service providers in the financial sector, utilities (electricity, water and gas), healthcare and passenger transportation, internet service providers, and other providers of critical activities (economic and/or social activity whose interruption has serious consequences on the health and safety of citizens, on the effective functioning of essential services that maintain the economy, society and government, or affects the economic and social prosperity in general) as well as educational services must comply with the following: (a) notifying the National Centre for Digital Security ('National Centre') about every digital security incident; and, (b) reporting and collaborating with the NDPA in case of a digital security incident that involves Personal Data.

## Enforcement

### At a glance

- 

---

The General Directorate of Sanctions (part of the NDPA) instructs on and resolves, in the first instance, violations and imposes sanctions as well as conducting and develops the research phase according to the applicable legislation.

The General Directorate for the Protection of personal data (also part of the NDPA) resolves in the second and last instance the sanctioning procedure and its decision exhausts the administrative route.

Possible sanctions for breaching data protection standards vary depending on the nature or magnitude of the offense:

- The fine applicable to minor infringement ranges from S/ 2,675 to S/ 26,750 (approximately between USD 720 and USD 7,200).
- The fine applicable to severe infringements ranges from S/ 26,750 to S/ 267,500 (approximately between USD 7,200 and USD 72,000).

- The fine applicable to very severe infringements ranges from S/ 267,500 to S/ 535,000 (approximately between USD 72,000 and USD 144,000).

## Electronic marketing

The PDPL does not expressly regulate electronic marketing. However, the PDPL does apply to electronic marketing activities if personal data is processed as a result.

If consent is obtained through electronic media, the notice requirements can be met by publishing accessible and identifiable privacy policies with the relevant consent language and mechanism. The PDPL establishes the possibility of obtaining express consent by presenting the option to agree with the privacy policies in clickable ways (eg , by clicking, ticking a box).

Written consent may be provided by other options, including:

- Through an electronic signature
- A written document possible to read or print
- A mechanism or procedure that allows one to identify the subject and to receive his consent through a written text
- A pre-established text as long as it is easily visible, legible and written in simple language

The laws governing electronic signatures are:

- Law N° 27291
- The Digital Certificates and Signatures Law (Law N° 27269)
- Supreme Decree N° 052-2008-PCM

Note that expressing the will in any of the regulated forms does not eliminate the other requirements of consent referring to that consent must be informed, and freely given.

According to the article 58.1 of Consumer Protection Code Law N° 29571, the following commercial activities require prior, informed, express and unequivocal consent to promote products and services:

- Use of call centers
- Use of telephone call systems
- Bulk text messages or
- emails Telemarketing services

As to date, it is permitted to obtain personal information from public sources or by licit means in order to contact the data subjects to get their consent for the aforementioned commercial activities. Notwithstanding the foregoing, whenever the data subject does not grant its consent for commercial activities, it must not be contacted again for those purposes. Furthermore, easily accessible and free

mechanisms must be implemented to allow the data subjects to revoke their consent for the commercial purposes.

However, a bill has been proposed, which would modify the aforementioned article 58.1, so that advertising could only be sent to consumers who request to receive such and grant the sender unequivocal, free, informed and express consent to be contacted for marketing purposes. So, a data subject's information (i.e. telephone numbers and e-mails) could be used for marketing purposes only if the data subject has consented to be contacted by the sender for marketing purposes.

## Online privacy

The New Regulation of the PDPL will be introducing some aspects regarding Online Privacy, including localization data as a category of personal data. Likewise, although it does not expressly regulate cookies the PDPL will apply if personal data is collected and processed using these mechanisms.

This requires that the use and deployment of cookies, location data or another personal data that will be collected must comply with data privacy laws. As a general rule, the data subject's consent must be obtained before cookies and/or location data can be used. Nevertheless, consent won't be necessary when an exception is in place. For example, regarding cookies, the NDPA considers that consent is not required for necessary cookies (i.e. those required for the functionalities of a webpage); however, consent will be required for marketing cookies (as they are not strictly required for the functionalities of a webpage but respond to a commercial purpose).

With respect to criminal law enforcement, Legislative Decree N° 1182 permits the National Police of Peru to access the location and geolocation of mobile phones or electronic devices of similar nature in cases of *flagrante delicto*.

It establishes the obligation for public communications services providers and public entities to keep the data from their users derived from telecommunication services during the first 12 months in computer systems an additional period of 24 months in an electronic storage system. Such service providers are bound to provide the location and geolocation data immediately, 24 hours a day, 365 days of the year, under warning of being liable to the responsibilities regarded by law in the event of noncompliance.

## Data protection lawyers



**Ricardo Escobar**

Partner  
DLA Piper  
[rescobar@dlapiper.pe](mailto:rescobar@dlapiper.pe)  
[View bio](#)



**Daniel Flores**

Partner  
DLA Piper  
[dflores@dlapiper.pe](mailto:dflores@dlapiper.pe)  
[View bio](#)

## For more information

---

To learn more about DLA Piper, visit [dlapiper.com](https://dlapiper.com) or contact:



### Carolyn Bigg

Partner  
Global Co-Chair Data, Privacy and  
Cybersecurity Group  
[carolyn.bigg@dlapiper.com](mailto:carolyn.bigg@dlapiper.com)  
[Full bio](#)



### John Magee

Partner  
Global Co-Chair Data, Privacy and  
Cybersecurity Group  
[john.magee@dlapiper.com](mailto:john.magee@dlapiper.com)  
[Full bio](#)



### Andrew Serwin

Partner  
Global Co-Chair Data, Privacy and  
Cybersecurity Group  
[andrew.serwin@us.dlapiper.com](mailto:andrew.serwin@us.dlapiper.com)  
[Full bio](#)

## About us

---

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

[dlapiper.com](https://dlapiper.com)